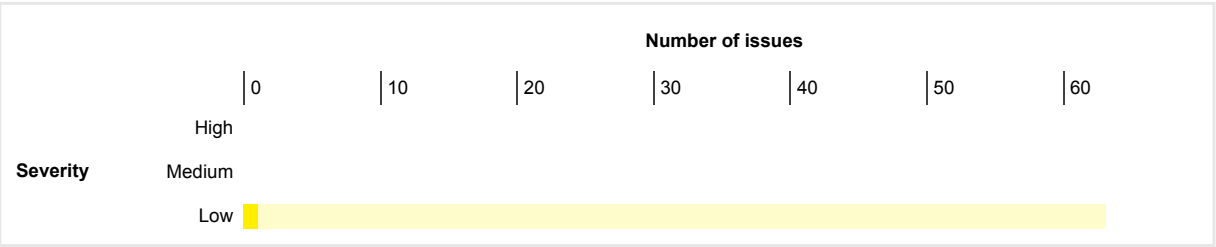
Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	1	0	62	63
	Information	3	2	0	5

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1.37. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.38. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.39. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.40. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.41. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.42. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.43. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.44. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.45. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.46. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp
1.47. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.48. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.49. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.50. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.51. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.52. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.53. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.54. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.55. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.56. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.57. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.58. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.59. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.60. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.61. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp
1.62. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

2. Strict transport security not enforced

3. Frameable response (potential Clickjacking)

3.1. https://192.168.1.193:7443/adeptia/forgotpassword.jsp
3.2. https://192.168.1.193:7843/Mapper/

4. Email addresses disclosed

4.1. https://192.168.1.193:7843/Mapper/rest/fetchproperties/serverconfigure
4.2. https://192.168.1.193:7843/pd/rest/fetchproperties/serverconfigure
4.3. https://192.168.1.193:7843/rest/fetchproperties/serverconfigure

---

1. Open redirection (DOM-based)

There are 62 instances of this issue:

- /adeptia/control/StartStopKernel.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp

- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

1.1. https://192.168.1.193:7443/adeptia/control/StartStopKernel.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/StartStopKernel.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/StartStopKernel.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFlQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=QueueProcessor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css t
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **kernel**.

The following value was injected into the source:

```
Pause Kernel
```

The previous value reached the sink as:

```
kernelStatus=qz1vo811ql%2527%2522`'"/qz1vo811ql/><qz1vo811ql/\>sgalliyvmo&
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at pauseKernel (https://192.168.1.193:7443/adeptia/control/js/ajax.js:3227:46)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/StartStopKernel.jsp:42:158)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at pauseKernel (https://192.168.1.193:7443/adeptia/control/js/ajax.js:3294:7)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/StartStopKernel.jsp:42:158)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **kernel** with the following HTML:

```
<input class="inputBgLink" onmouseover="this.style.cursor='pointer'" type="button" name="kernel" val
```

1.2. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
```

```
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:59:60)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.3. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckctySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:58:64)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.4. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:57:58)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.5. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:56:62)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.6. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFlQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
```

```
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:63:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.7. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
```

```
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVlZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:62:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.8. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:61:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.9. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
```

```
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:60:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.10. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:59:60)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.11. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
```

```
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:58:64)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.12. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:57:58)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.13. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
```

2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=juipljw3j9%2527%2522`'"/juipljw3j9/><juipljw3j9/\>zd1ngl4kwh&&endDate=aogzbbswip%2527%2522`'"/aogzbbswip/><aogzbbswip/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:56:62)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:2559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.14. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity: **Low**

Confidence: **Tentative**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:63:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
```

```
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.15. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:62:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.16. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
```

ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=datainterfaceslog.jsp

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:61:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.17. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=datainterfaceslog.jsp
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=awvqkfemoe%2527%2522`'"/awvqkfemoe/><awvqkfemoe/\>olt72c1od7&&endDate=flqdgf82od%2527%2522`'"/flqdgf82od/><flqdgf82od/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
```

```
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:60:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getEventMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:2279:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:64:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:71:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp:120:497)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.18. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckctySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:165:64)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.19. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:164:58)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.20. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:163:62)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.21. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
```

```
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **secondTablePgno**.

The following value was injected into the source:

```
1
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:172:61)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.22. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
```

```
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
Sckty SFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **firstTablePgno**.

The following value was injected into the source:

```
1
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:171:59)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.23. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:170:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.24. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
```

```
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:169:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.25. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:168:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.26. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
```

```
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:167:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.27. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvbIBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:166:60)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.28. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
```

```
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:165:64)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.29. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:164:58)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
```

```
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.30. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckctySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

```
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=si7eyywkhp%2527%2522`'"/si7eyywkhp/><si7eyywkhp/\>eib2is52j7&&endDate=pfditae5m9%2527%2522`'"/pfditae5m9/><pfditae5m9/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:163:62)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:2556)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.31. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
```

eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **firstTablePgno**.

The following value was injected into the source:

```
1
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:171:59)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.32. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity: **Low**

Confidence: **Tentative**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request


```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckctySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVlZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFlQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```


Response


```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```


Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:170:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.33. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:169:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.34. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
```

```
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIIFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:168:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.35. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**

Path: **/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:167:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.36. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:166:60)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.37. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
```

```
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:165:64)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.38. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request


```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```


Response


```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```


Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:164:58)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.39. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
userTypeId=&startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:163:62)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUserRoleTaskInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1184:7)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:179:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.40. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
```

```
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **secondTablePgno**.

The following value was injected into the source:

```
1
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:172:61)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.41. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **firstTablePgno**.

The following value was injected into the source:

```
1
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:171:59)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.42. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:170:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.43. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
```

```
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUElI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:169:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.44. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**

Path: **/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:168:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.45. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:167:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.46. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
```

```
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUElI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFlQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=SolutionMonitor
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=puq39p98no%2527%2522`'"/puq39p98no/><puq39p98no/\>tbwvftvn79&&endDate=do4144myj4%2527%2522`'"/do4144myj4/><do4144myj4/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:166:60)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getPerformanceMonitorDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1304:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:173:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:178:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp:22:494)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.47. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**

Path: **/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:59:64)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.48. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:58:58)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.49. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
```

```
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUElI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/01/2019
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:57:62)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.50. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**

Path: **/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:64:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.51. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request


```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```


Response


```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:63:50)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.52. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
```

```
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:62:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.53. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVlekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:61:54)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
```

```
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.54. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request


```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```


Response


```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```


Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:60:60)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.55. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartHours**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:59:64)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.56. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUElI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndDate**.

The following value was injected into the source:

```
08/08/2019
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:58:58)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.57. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
Sckty SFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempStartDate**.

The following value was injected into the source:

```
08/01/2019
```

The previous value reached the sink as:

```
startDate=ltbfb2rq0i%2527%2522`'"/ltbfb2rq0i/><ltbfb2rq0i/\>htmefarge4&&endDate=xmkrpwg75e%2527%2522`'"/xmkrpwg75e/><xmkrpwg75e/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:57:62)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at HTMLInputElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:2621)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event on an element with a name of **cancel** with the following HTML:

```
<input class="button" type="button" name="cancel" value="Cancel" onclick="closeAndCencelForDate();">
```

1.58. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVlekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODIXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
```

```
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endSecs**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:64:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.59. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVlekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **endMins**.

The following value was injected into the source:

```
59
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:63:50)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.60. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVlekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startSecs**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:62:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.61. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
```

```
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **startMins**.

The following value was injected into the source:

```
00
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:61:54)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

1.62. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVlekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckytySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6;
lastService=IndigoReportLimited
```

Response

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has name **tempEndHours**.

The following value was injected into the source:

```
23
```

The previous value reached the sink as:

```
startDate=v4koyob1fk%2527%2522`'"/v4koyob1fk/><v4koyob1fk/\>rar4h901fj&&endDate=nc1v3xsbrf%2527%2522`'"/nc1v3xsbrf/><nc1v3xsbrf/\
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:1170364)
at HTMLInputElement.get [as value] (<anonymous>:1:1272851)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:60:60)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

The stack trace at the sink was:

```
at Object.GEKsW (<anonymous>:1:426038)
at Object.KHJWD (<anonymous>:1:1222291)
at XMLHttpRequest._0x2e8d12.<computed>.<computed>.send (<anonymous>:1:1241324)
at getUsageReportDateInfo (https://192.168.1.193:7443/adeptia/control/js/ajax.js:1492:7)
at closeAndCencelForDate (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:65:2)
at refreshAllTables (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:72:2)
at HTMLAnchorElement.onclick (https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp:106:559)
at _0x7dec10 (<anonymous>:1:1383446)
at Object.UZtdW (<anonymous>:1:437816)
at _0x2505e3 (<anonymous>:1:1397344)
```

This was triggered by a **click** event with the following HTML:

```
<a href="JavaScript:void(0)" onclick="refreshAllTables();"><img src="/adeptia/icons/arrow_refresh.gi
```

---

2. Strict transport security not enforced

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials

Request

```
GET /Mapper/ HTTP/1.1
Host: 192.168.1.193:7843
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7843/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
SckctySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZIY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEl1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=SAPLogs;
JSESSIONID=node0rr4y80i0qg78eurgvts9tl2.node0
```

Response

```
HTTP/1.1 200
Accept-Ranges: bytes
ETag: W/"108019-1565105614000"
Last-Modified: Tue, 06 Aug 2019 15:33:34 GMT
vary: accept-encoding
Content-Type: text/html
Date: Thu, 08 Aug 2019 06:33:21 GMT
Connection: close
Server: Adeptia
Content-Length: 108019

<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-
...[SNIP]...
```

---

3. Frameable response (potential Clickjacking)

There are 2 instances of this issue:

- https://192.168.1.193:7443/adeptia/forgotpassword.jsp
- https://192.168.1.193:7843/Mapper/

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure

3.1. https://192.168.1.193:7443/adeptia/forgotpassword.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/forgotpassword.jsp**

Request

```
GET /adeptia/forgotpassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
```

```
Connection: close
```

Response

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0rlm2t130axic10ljoehjfy5672134.node0; Path=/adeptia; Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 414


<html>
<title>Recover Password</title>
<head>
      <link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
</head>
<body>
    <!--    <
...[SNIP]...
```

3.2. https://192.168.1.193:7843/Mapper/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7843**
Path:	**/Mapper/**

Request

```
GET /Mapper/ HTTP/1.1
Host: 192.168.1.193:7843
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7843/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoVC9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl
2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWll1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBw
WQ0KdDVZUERkVWlxd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktweWJuUQ0KbWU2dFFTdXVO
ZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsOWRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2
eWkrZ1AwL0wxRjNScTB5N1hndGNaQWtmT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nTGNXUE
1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY21sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJ
ScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRRaE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBh
bg0KQWpSRWpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnRWeDhuYzNTbQ0KVWxBaDZYWW
pRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURNNjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRm
Q3bmV0cEF0cnptYnNBZTdmeGQvTys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQkVtNitGeHpG
RGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1
MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuoVilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=SAPLogs;
JSESSIONID=node0rr4y80i0qg78eurgvts9tl2.node0
```

Response

```
HTTP/1.1 200
Accept-Ranges: bytes
ETag: W/"108019-1565105614000"
Last-Modified: Tue, 06 Aug 2019 15:33:34 GMT
vary: accept-encoding
Content-Type: text/html
Date: Thu, 08 Aug 2019 06:33:21 GMT
Connection: close
```

```
Server: Adeptia
Content-Length: 108019

<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-
...[SNIP]...
```

---

4. Email addresses disclosed

There are 3 instances of this issue:

- /Mapper/rest/fetchproperties/serverconfigure
- /pd/rest/fetchproperties/serverconfigure
- /rest/fetchproperties/serverconfigure

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

Vulnerability classifications

- CWE-200: Information Exposure

4.1. https://192.168.1.193:7843/Mapper/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/Mapper/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request

```
GET /Mapper/rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response

```
HTTP/1.1 200
Connection: close
X-Powered-By: Adeptia Connect
```

```
Cache-Control: no-cache
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
vary: accept-encoding
Content-Type: text/plain
Date: Tue, 04 May 2021 06:22:13 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forcedSAMLIDPLogoutEnabled":true,"characterSetE
ncoding":"UTF-8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia.com","productName":"Adeptia
Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebPdAutoSaveEnabled":true,"acPortsJson":"
{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```

4.2. https://192.168.1.193:7843/pd/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/pd/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request

```
GET /pd/rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response

```
HTTP/1.1 200
Connection: close
X-Powered-By: Adeptia Connect
Cache-Control: no-cache
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
vary: accept-encoding
Content-Type: text/plain
Date: Tue, 04 May 2021 06:22:15 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forcedSAMLIDPLogoutEnabled":true,"characterSetE
ncoding":"UTF-8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia.com","productName":"Adeptia
Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebPdAutoSaveEnabled":true,"acPortsJson":"
{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```

4.3. https://192.168.1.193:7843/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**

Confidence: **Certain**

Host: **https://192.168.1.193:7843**

Path: **/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request

```
GET /rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response

```
HTTP/1.1 200
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Connection: close
Expires: 0
Pragma: no-cache
X-Powered-By: Adeptia Connect
vary: accept-encoding
Content-Type: text/plain
Date: Tue, 04 May 2021 06:22:18 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forcedSAMLIDPLogoutEnabled":true,"characterSetEncoding":"UTF-8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia.com","productName":"Adeptia Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebPdAutoSaveEnabled":true,"acPortsJson":"
{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```
